R926, Acceptable Use of Office-owned IT Resources[1]

R926-1. Purpose: To require appropriate use of office owned IT resources for official work of the office and to maintain appropriate separation between such office use and personal or entertainment use of such resources. This policy applies to both internal and external access, and encompasses, but is not limited to OCHE resources such as computers, laptops, servers, workstations, networks, computer programs, databases, storage devices, media, printers, photocopiers, facsimile machines, peripheral equipment, gateways, intranets, internet access, web sites, e-mail, telephones, personal digital assistants, wireless devices, voice-mail, other communication devices, and digital and electronic information and data.

R926-2. References

2.1. Policy and Procedures R345, Information Technology Resource Security

2.2. Policy and Procedures R927, Use and Security of Property

2.3. Policy and Procedures R951, Staff Employee Grievances

2.4. Policy and Procedures R952, Discrimination and Sexual Harassment Complaints

2.5. Policy and Procedures R964, Corrective Action and Termination of Staff Personnel

2.6. Policy and Procedures R992, Information and Technology Resource Security

2.7. Policy and Procedures R993, Records Access and Management

R926-3. Office-owned IT Equipment and Software Policy

3.1. Use of Office Owned IT Resources: Office-owned IT Resources, including desktop and portable PCs, is subject to the general Office of the Commissioner of Higher Education (OCHE) policy R927 regarding personal use of office facilities and equipment. The equipment, installed software on the equipment, and any access to the Internet, are provided for purposes of the official work of the office, not for personal use or entertainment. Staff members are expected and required to use office owned equipment primarily for official business in connection with their jobs. Staff members are expected and required to spend on duty time (which does not include break time and lunch time) on official business in connection with their jobs and not on personal affairs or entertainment. This expectation is of course qualified by normal allowance for emergencies that might arise and for reasonable and incidental socializing that facilitates effective working relationships. The same expectation and requirement applies to use of office owned IT Resources -- that is, the IT Resources are to be used principally for official business purposes related to the staff member's specific job.

3.1.1. The Office retains the right to allocate its information resources and to control access to its electronic communications systems.

3.2. Use During Break Time, During Travel, or at Home: During break time or in the case of portable equipment used at home or in travel status, the office policy does not prohibit incidental personal use of the

[1] Approved August 3, 2000; amended October 31, 2003, October 26, 2006 and May 30, 2008.

equipment, subject to the provisions set forth below. However, “incidental” is to be interpreted literally, meaning in this case a very small portion of the total use of the equipment. As a singular exception to this provision, job related training or other approved course enrollments are considered to be job related activity. Staff members are required to exercise reasonable precautions in caring for any equipment authorized for use off premises, and are personally responsible for any damage resulting from use by family members or unauthorized persons. Incidental personal use might include such activities as:

3.2.1. Using the office phone on occasion to make necessary calls (see R926-5 below for details).

3.2.2. Faxing an important document if necessary (e.g., faxing information to a mortgage company during the home purchase process).

3.2.3. Accessing the Internet for reasonable and appropriate personal use, for educational or research projects, to retrieve news stories or other information of general interest, to participate in professional or civic organizations, or to perform nonprofit or community service.

3.2.4. Using e-mail to send occasional brief messages to recipients outside OCHE or to receive such messages.

3.2.5. Storing a limited amount of appropriate types of personal non executable files on one's local computer hard drive (C:). (Local drives may be changed or re-imaged at any time, thus making files inaccessible.)

3.3. Authorization and Installation of Software: Without exception, software installed on office owned IT Resources equipment is required to be owned by the office and installed by Computer Services (CS) staff members. Installation of personal copies of software or installation of software (including but not limited to computer games) by other staff members is prohibited. This policy is intended to ensure compliance with software licensing obligations and also to safeguard against avoidable introduction of computer viruses, as well as avoiding unnecessary potential overloading of memory and hard disc storage capacity of office owned equipment. Need for specific specialized software packages (apart from the office wide standard software modules installed as authorized by cognizant Associate Commissioners or UHEAA Associate Executive Directors) may be verified in writing by the cognizant Associate Commissioner or Associate Executive Director and will then be purchased and charged to the applicable cost center budget in OCHE or UHEAA, and installed by CS. CS staff are instructed to remove games from any currently installed software and from new software as installed. If unauthorized software is found on office owned equipment, CS staff are under a standing instruction to delete it. CS has available a variety of options for PC wallpaper and screen saver applications, and individual staff members may contact CS at their option to select personal choices from the available options. Persons with Internet access on office owned IT Resources may download documents related to their official duties, but are prohibited from downloading any software without first checking with CS to ensure both compliance with licensing requirements and protection against interference with other installed software. Persons downloading job related documents are required to pay close attention to any warnings from CS regarding potentially harmful documents.

3.4. Prohibition on Copying Office installed Software: Under no circumstances may individual staff members copy office owned software for installation on personal or any other computer equipment. In some cases, staff members wishing to work at home on office business, either on their own time or on an approved telecommuting basis, may wish to utilize personally owned computer equipment. With specific approval by the cognizant Associate Commissioner or Associate Executive Director, related office owned software may be installed on the staff member’s personal computer equipment, but only by CS staff members. An inventory of office owned software installed on staff members’ personal PCs will be

maintained, and the software will be required to be deleted and the deletion verified when a staff member leaves employment with the organization.

3.6. Internet Access and Use: Staff members are expected to exercise sound judgment in limiting their use of internet access to official business related purposes during normal business hours. Any personal uses of office provided Internet capacity must be strictly incidental (as defined in 3.1), limited to breaks, lunch hour, or other off duty time, and in keeping with standards of ethical behavior. Staff members with off premises access to the Internet through the office dial-up network are required to safeguard against its use by unauthorized persons. CS staff are instructed to monitor and periodically check the sites addressed using office Internet access.

3.7. Web logs (Blogs), Chat Rooms, Bulletin Boards: Personal blogs, chat rooms or bulletin boards may not be hosted on the OCHE network. A blog is a journal (or newsletter) that is frequently updated and intended for general public consumption. Blogs generally represent the personality of the author or the Web site. OCHE employees are discouraged from publicly discussing work related matters, whether constituting confidential information or not, outside of appropriate work channels, including online in chat rooms, on bulletin boards, or in their personal blogs. An employee with a blog or who participates in a chat room or a bulletin board must:

3.7.1. Make it clear that the views expressed are the employee's alone and do not necessarily represent the views of OCHE.

3.7.2. Respect OCHE's confidentiality and proprietary information.

3.7.3. Ask his/her manager if there are any questions about what is appropriate to include in a blog, bulletin board or chat room.

3.7.4. Be respectful to OCHE, OCHE employees, customers, partners, and competitors.

3.7.5. Understand and comply when OCHE asks that topics not be discussed for confidentiality or legal compliance reasons.

3.7.6. Ensure that blogging, chatting, or bulletin board activities do not interfere with OCHE work commitments.

R926-4. Electronic Messaging Policy

4.1. Use of the Messaging System: The OCHE Messaging System consisting of e-mail/calendaring client software, e-mail/calendaring servers, and supporting infrastructure is the property of OCHE and should be used for legitimate administrative purposes. Users are permitted access to the Messaging System to assist them in performing their role within OCHE. Use of the Messaging System is a privilege that can be revoked at any time.

4.2. Passwords: Users are responsible for safeguarding their passwords. Individual passwords should not be printed, stored online, or given to others (including family members). (See R992.4.5 User Authentication.)

4.3. Separation from OCHE: Supervisors may request CS to retrieve personal e-mails and other personal electronic data from an employee's e-mail account prior to the employee's separation from OCHE.

4.4. Delegated (Proxy) Access: A User may grant delegated (proxy) access to another user in the e-mail system. Requests for delegated (proxy) access must be approved by the User whose account will be accessed. (See R992.4.6 for provisions to arrange such access.)

4.4.1. Individuals who request access to another person's e-mail, and receive approval to do so, will not receive permission to directly access the e-mail account, but will be allowed to choose e-mail messages they would like printed or forwarded to them that directly relate to the issue described in their request for access.

4.5. Users Responsible for Messages: Users are responsible for any messages sent or forwarded from their e-mail account.

4.6. Distribution or Storage of Prohibited Materials: Without prior written permission from the cognizant Associate Commissioner, e-mail may not be used for dissemination or storage of commercial or personal advertisements, solicitations, promotions, destructive programs (i.e., viruses), or any other unauthorized use.

4.7. Waste of Messaging System Resources: Users may not deliberately perform acts that waste Messaging System resources or unfairly monopolize resources to the exclusion of others. These acts include, but are not limited to, mass mailings, chain letters, multiple copies of documents, or otherwise creating unnecessary network traffic. The administrators of the OCHE Messaging System reserve the right to disable mailboxes that are creating system wide problems.

4.7.1. Users may not initiate or forward chain messages. Chain messages are defined as messages sent to a number of people asking each recipient to send copies of the same request to a number of other recipients.

4.7.2. Mass e-mail is a message that is sent to a large number of recipients. All mass e-mail must be approved before dissemination. Approval must be granted by the cognizant Associate Commissioner or his/her designee.

4.8. Personal Use: Incidental personal use is allowed as long as it does not interfere with the operation of the e-mail system and does not provide an added burden for OCHE Messaging System administration.

4.9. Account Management: CS has primary responsibility for the OCHE Messaging System. Accounts are available only to current staff of OCHE. Special consideration may be made for outside affiliates and consultants.

4.9.1. All Messaging System Users must have signed the Security and Confidentiality agreements and must have reviewed this e-mail policy.

4.9.2. The Messaging System User ID must be unique and in the form of an OCHE ID as issued by OCHE. The canonical e-mail address for a User will be based on the Messaging System User ID. Exceptions will be allowed for work group resources (conference rooms, equipment, and generic work group e-mail address).

4.9.3. An e-mail account will be limited to a quota set by OCHE guideline, however exemptions are possible with demonstrated need and approval by the cognizant Associate Commissioner. Users will be responsible to manage their personal storage space to keep it below the quotas. Users will be provided with mechanisms to archive e-mail. The archiving method used will be determined by work unit security and retention requirements. If an employee's mailbox size

exceeds the storage limitation and remains above the specified limitation, users will be unable to create new messages. However, user's ability to receive new messages will NOT be affected.

4.9.4. No User will be allowed more than one Mailbox in the messaging system.

4.10. Mail Retention and Backup: E-mail backup and retention guidelines will be based on a documented risk assessment, as set by the Information Technology Council established by R992.

4.11. Internet Mail: Internet addresses will be in the form determined by the Information Technology Council. The security of messages sent outside the e-mail system (via the Internet or otherwise) cannot be guaranteed. Users shall not send e-mail containing information considered to be sensitive or confidential.

4.11.1. Delivery of e-mail messages (including delivery in a timely fashion) to recipients outside of the e-mail system cannot be guaranteed. Internet mail messages have up to 24 hours to reach their destination. Users should receive a notification of any bounced messages.

4.11.2. E-mail messages are limited to a maximum size of 25 MB including attachments.

4.11.3. Due to spam and virus propagation, certain attachments are quarantined or blocked. The following types of files that are examples of blocked or quarantined attached messages when sent as an attachment: .exe, .scr, .pif, .cmd, .cpl, and .hta. CS can provide a list of blocked or quarantined attachments.

4.12. Blocking: CS uses blocking products containing lists of IP addresses of known sources of unsolicited commercial and bulk e-mail (a.k.a. spam) in the attempt to minimize and manage the impact of spam on the OCHE Messaging System.

4.13. E-Mail Access and PDA Software Support: Users are provided a variety of supported ways to access their e-mail. PDA's (Personal Digital Assistant/Handheld computer), in addition to a variety of other features, let users synchronize with the OCHE e-mail system. Standard server facilities will be provided for PDA integration.

4.14. E-Mail Discontinuance: E-mail accounts will be removed from the system when CS receives termination notification from Human Resources.

4.15. Disclaimer: E-mail users and those in possession of OCHE records in the form of electronic mail are cautioned to be prudent in their reliance on electronic mail for purposes of maintaining a lasting record. Sound business practice suggests that consideration be given to transferring (if possible) electronic mail to a more lasting medium/format, such as acid free paper or microfilm, where long term accessibility is an issue.

4.15.1. Due to the nature of e-mail, the storage and delivery of e-mail cannot be guaranteed.

R926-5. Telephone Policy

5.1. Use of Telephone Systems: The OCHE telephone systems and equipment are provided for the conduct of official business. Use of these facilities for personal business should be kept to a minimum.

5.1.1. Call center phones are subject to monitoring and recording. Usage reports can be generated for all OCHE phones and may be monitored for abnormally high usage volumes.

5.1.2. Office telephone numbers should never be formally published in connection with personal business. OCHE's 1-800 numbers should not be given out for incoming personal calls. These phone numbers are strictly for the use of OCHE's clients, or prospective clients, to be used when contacting OCHE about official business.

5.2. Long Distance and Toll Calls: Long distance and other toll calls for private business made through the OCHE telephone system should be charged to the individual's home telephone or personal calling card. If this is not possible, a record of private calls made at OCHE expense must be kept and repayment must be made upon receipt of the telephone bill. Supervisors are responsible to prevent abuse and ensure that repayment is made. Personal collect calls should not be accepted.

5.3. Allowance for Personal Cellular Telephones: If an employee requires a cellular phone in order to perform his/her duties, the employee, with approval of the cognizant Associate Commissioner or designee, will obtain a personal cellular access plan and cellular phone and will receive an allowance from OCHE via additional compensation, within approved limits. The additional compensation must be justified by business requirements which necessitate the use of a cellular telephone to perform official OCHE business where such business cannot be accommodated by the use of a land line phone, pager, or other less expensive communication device. The cellular telephone is owned by the employee and may be used for personal business. The approved allowance amount must be based on business requirements. The employee may, at his/her own expense, elect to purchase additional service(s). Approved procedures must be followed when providing additional compensation for this purpose.

5.4. OCHE Owned Cellular Telephones- OCHE shall not purchase or own cellular telephones except in those circumstances where employee ownership of the cellular plan and telephone is not practicable as determined by the cognizant Associate Commissioner. OCHE owned cellular telephones provided for the conduct of official business shall not be used for personal business.

5.4.1. IRS published authority defines requirements for adequate substantiation of the business use of OCHE owned cellular telephones. Unsubstantiated cellular use may be deemed personal use and therefore considered wages subject to employment taxes.

5.4.2. Adequate substantiation of business use includes the time, date, place, business purpose, and amount of the expense. Substantiation of business use should be in the format of a record or log made at or near the time the telephone call was placed.

5.4.3. An employee shall repay OCHE for incoming and outgoing personal use of an OCHE owned cellular phone. The reimbursement amount shall include direct charges for personal use and a pro rata share of monthly fees and services. Supervisors are responsible to prevent abuse and ensure that repayment is made.

5.4.4. If a user is not able or willing to comply with IRS substantiation requirements for OCHE owned cellular services and devices, the department or individual must use the individual ownership option described in paragraph 5.3.

5.5. No Cellular Use while Operating a Motor Vehicle: Employees shall not use cellular telephones to conduct the business of OCHE while operating a motor vehicle.

R926-6. Privacy, Security and Monitoring Policy

6.1. Privacy and Security: Users shall respect the legitimate expectations of privacy of others. However, appropriate administrators and network managers may require access to users' e-mail and other

electronic records typically taken to be private. In particular, individuals having electronic communication system administration responsibilities, who cannot perform their work without access to e-mail and other records in the possession of others, may access such information as needed for their job responsibilities.

6.1.1. Users shall treat institutional data, files maintained by other Users as confidential unless otherwise classified pursuant to state or federal statutes, regulation, law or Board policy. Users shall not access files or documents belonging to others, without proper authorization or unless pursuant to routine system administration.

6.1.2. Users shall not knowingly falsely identify themselves and will take steps to correct misrepresentations if they have mistakenly falsely identified themselves.

6.2. No Guarantee of Security or Privacy: The security and privacy of electronic records cannot be guaranteed. During the course of system maintenance, IT Resources staff may view the contents of records as they are processed through the electronic communications system. However, these staff members are expected to maintain the confidentiality of any data they encounter in accordance with R992. Not doing so may subject IT Resources administrators to disciplinary action up to and including termination.

6.3. Security Limitations: Electronic communications systems have inherent limitations. No computer security system can absolutely prevent a determined person from accessing stored information that he/she is not authorized to access. Moreover, electronic documents may be disclosed pursuant to public records law or in the discovery process. Users should not consider e-mail to be private or secure. Messages addressed to nonexistent or incorrect user names may be delivered to unintended recipients.

6.4. Prohibited Activities: Any activity that violates OCHE's Information Resources Policy (R992) or generally accepted standards of computer ethics and etiquette is prohibited. Services associated with the computers, software, and electronic communication systems will not be used for illegal or improper purposes. This includes, but is not limited to, the generation of threatening, harassing, abusive, obscene or fraudulent messages. The use of the OCHE Systems must comply with this policy and applicable Federal and State Law. IT Resources may not be used in a manner that involves or facilitates any of the following prohibited uses:

6.4.1. Any infringement or misappropriation of copyrighted material or software, trade secrets or other intellectual property;

6.4.2. Any attempt to gain or help others gain access without authorization or anything that jeopardizes the security of IT Resources, data, or confidential information, or the privacy rights of others;

6.4.3. Engaging in or facilitating any crime, fraud, or illegal act, including gambling and sports pools;

6.4.4. Racist, sexist, stalking, harassing, or threatening communications (See R954, Sexual Harassment and Consensual Relationships.);

6.4.5. Any use that is for personal gain of the employee or another person, including selling access to their User ID's, political activity, personal business, or commercial enterprise or to solicit for charitable organizations not approved and sponsored by OCHE;

6.4.6. Any misrepresentation of the identity of the sender, including sending a message as an official OCHE communication without appropriate permission;

6.4.7. Distribution, communication, access, download or display of pornography or material that is sexually explicit, excessively violent, harassing or otherwise offensive;

6.4.8. Destruction, damage or alteration to any Office IT Resource or property without proper authorization or any unauthorized change to the design or configuration of IT Resources, including the installation of non OCHE approved screen savers or downloading executable software that is not approved by CS;

6.4.9. Any unauthorized activity that interferes with or adversely affects the performance of the employee's work or the work or responsibilities of others using OCHE's networks and systems, such as implementing or propagating a computer virus, using destructive software, inappropriate game playing, or monopolizing information resources for entertainment or personal use;

6.4.10. Sending or forwarding unsolicited bulk e-mail, chain letters, or "spam";

6.4.11. Any attempt to circumvent or disable security, monitoring, filtering, or auditing software or systems of OCHE or engage in any activity that might be harmful to systems or information stored thereon or interfere with the operation thereof by disrupting services or damaging files. Examples include but are not limited to: running "password cracking" programs, attempting to read or change administrative or security files or attempting to or running administrative programs for which permission has not been granted, using a telnet program to connect to system ports other than those intended for telnet, using false identification on a computer or system or using an account assigned to another, forging mail or news messages; or

6.4.12. Any attempt to monitor or tamper with another user's electronic communications or copy, change, or delete another user's files or software without the explicit agreement of the owner(s).

6.5. Monitoring: OCHE reserves the right but does not have the duty, to monitor any and all aspects of its IT Resources system. OCHE does not monitor IT Resources as a routine matter, but it will do so, to the extent permitted by law, when OCHE deems it necessary for purposes of maintaining the integrity and effective operation of the IT Resources systems or to evaluate job performance quality (See R992-5.1.4 and 5.1.8 for information security monitoring). Also, there are cases where “responsive monitoring” is performed whereby OCHE monitors in response to a particular problem, complaint, investigation to a claim or lawsuit. Such responsive monitoring will be approved by Human Resources and the cognizant Associate Commissioner. Monitoring will comply with the following restrictions:

6.5.1. All monitoring will be relevant to a particular OCHE purpose, problem, complaint, investigation of a claim, or lawsuit;

6.5.2. Disclosure and use of resulting data will be restricted to OCHE related purposes;

6.5.3. Monitoring a person's e-mail must be approved by Human Resources and the cognizant Associate Commissioner; and

6.5.4. Advice from legal counsel may be sought before permission to monitor is granted.

6.6. Monitoring Activities: In order to conduct its monitoring activities OCHE may:

6.6.1. Record Call Center phones used by telephone associates;

6.6.2. Generate telephone usage reports;

6.6.3. Review computer and network usage;

6.6.4. Scan, review, and record incoming/outgoing e-mail and instant message activity;

6.6.5. Track every instance of Internet connection;

6.6.6. Review system resource usage logs including disk space, remote access, log-in and other system logs.

R926-7. Disciplinary Action Policy

7.1. Report Non-compliance: Incidents of actual or suspected non-compliance with this policy should be reported to the appropriate authorities.

7.2. Suspension of Access: A systems administrator may immediately suspend the access of a User when the administrator reasonably believes:

7.2.1. the User has violated Office policies or law; and

7.2.2. the User's continuing use of Information Resources will result in: (1) damage to the Information Resources systems, (2) further violations of law or policy or (3) the destruction of evidence of such a violation.

The User shall be informed of his/her right to immediately appeal such a suspension to the cognizant head of the department or unit. Permanent revocation of privileges shall be imposed solely through the disciplinary processes set forth in paragraph 7.3. Users who are not USHE employees may have their access to IT Resources unilaterally revoked if they violate this policy.

7.3. Disciplinary Action: Personal use of OCHE's It Resources is a privilege rather than a right. Staff members using the systems in an appropriate manner and on an occasional personal basis need not be concerned about monitoring activities or possible disciplinary actions. However, misuse of any of these systems or other violation of this policy may subject a staff member to disciplinary action up to and including termination of employment in accordance with policy R964, Corrective Action and Termination of Staff Personnel.